移动云环境下高效属性基加密方案研究 *

付雨萌，孙　磊，李作辉

(信息工程大学，郑州 450001)

摘　要：随着云计算的普及，移动设备可以随时随地存储和检索个人数据。属性基加密(attribute based encryption，ABE)可用来解决移动云数据安全问题。目前适应移动云的属性基加密研究主要集中在单一机构，并不满足现实中的属性授权情况。针对以上问题提出了一个新的多机构属性基加密方案，该方案无中央权威，各授权机构可互不影响，分发的属性可添加；利用预计算、外包解密的方法降低用户端的计算开销；方案在随机预言模型下证明是静态安全的。实验结果表明，移动端在云环境下实施数据共享时，该方案可以减少移动设备端 20%的计算开销，更符合于移动云环境实际应用场景。

关键词：移动云计算；属性基加密；外包；多授权中心

中图分类号：TP309　　doi: 10.3969/j.issn.1001-3695.2018.03.0221

Efficient decentralizing ABE for mobile cloud computing

Fu Yumeng, Sun Lei, Li Zuohui

(*Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: With the popularity of cloud computing, mobile devices can store and retrieve personal data anytime and anywhere. Attribute based encryption can be used to solve the problem of mobile cloud data security. At present, the research on attribute based encryption adapting to mobile cloud is mainly focused on single authority, which does not satisfy the real property authorization situation. This paper proposed a new multi-authority attribute based encryption scheme with no central authority, each authority in the scheme could not affect each other and attributes could be added independently. In addition, the scheme uses precomputation and outsourcing decryption to reduce the computation cost of the user side. Besides, the scheme was static secure under the random oracle model. Experimental results show that the scheme can reduce the computation cost of the user side by 20%, and it is more consistent with the data sharing application scenario in the mobile cloud environment.

Key words: mobile cloud computing; attribute based encryption; outsourcing; multi-authority

0　引言

移动云计算(mobile cloud computing, MCC)[1~3]的产生使云计算获得了应用范围上的极大扩展，用户可以摆脱时间和空间的限制，更加便捷地享有云端强大的计算、存储和软件服务能力。目前国内外著名企业相继提供了移动云计算服务，如阿里在 2017 年重磅发布的移动云 Apsara Mobile、苹果公司“MobileMe”服务、微软公司“LiveMesh ”等。伴随移动设备的普及和 5G 网络的快速发展，移动云成为了近两年来关注的热点。同时，云计算的安全问题也逐渐得到关注，2017 年 Gartner 公司提出云安全成熟度曲线[4]指出面向云计算的环境数据、应用程序和工作负载安全防护参差不齐，移动设备的数据防护不够成熟，云安全的相关解决方案并不能直接应用于移动云环境。

属性基加密体制较好地解决了传统加密手段难以与多个用户实施灵活共享的问题，在云环境数据共享安全方面表现出色。但由于目前提出的大多方案都建立在双线性映射技术的基础之上，庞大的双线性对和群幂运算效率问题一直倍受研究者们诟病。

本文提出了一种适用于移动云环境的无中心属性基加密方案，主要优势体现在以下几个方面：

a)利用在线/离线、解密外包等技术将部分计算迁移到云端，使移动端用户加、解密时只需各完成一次指数运算，对移动端设备性能要求低，更符合移动云应用场景；

b)基于 LSSS(linear secret sharing schemes)访问结构构建方案，实现了更强的表达能力和更高的效率；

收稿日期：2018-03-26；**修回日期：**2018-05-11　　**基金项目：**国家重点研发计划资助项目（2016YFB0501900）

作者简介：付雨萌（1990-），女，新疆乌鲁木齐人，助教，硕士研究生，主要研究方向为云计算安全与属性加密（250609564@qq.com）；孙磊（1973-），男，教授，博士研究生，主要研究方向为云计算、信息安全、云计算基础设施可信增强、可信虚拟化技术；李作辉（1981-），男，副研究员，博士研究生，主要研究方向为公钥密码学、网络安全.

c)方案构建中引入映射思想，在属性与机构之间建立满射，符合管理实际，减少来自同一机构授权属性的密钥计算消耗；在属性与群元素之间建立一一映射，满足后续随时添加属性而不会影响整体方案运行需要；

d)方案在随机预言模型下证明是静态安全的。

1　相关工作

移动云计算一般可以概括为移动终端通过无线网络，以按需、易扩展的方式从云端获得所需的基础设施、平台、软件等资源或信息服务的使用与交付模式[5]。移动云计算 2010 年提出以来，移动云安全就受到了学者们广泛关注[6~8]：文献[6]提出移动云存储关键词搜索加密方案，文献[7]提出移动云医疗隐藏访问结构的外包属性基加密方案，文献[8]着重介绍目前为确保移动云计算基础设施安全而开展的最新工作，总结了安全问题对于移动云计算发展的重要性。

目前对于云计算安全较好的解决方法是采用属性基加密技术，能同时提供云数据安全和灵活地访问控制，但典型的 ABE 方案无法直接投入实际应用，原因在于方案需要利用双线性映射技术构建，复杂的功能性依靠一些模幂运算或双线性对运算实现，效率很难突破。2011 年，Green 等人[9]将外包思想引入 ABE，利用云端强大的计算和存储能力解决 ABE 性能瓶颈问题，把复杂的解密计算进行安全外包，为之后的研究提供了新思路。随后学者们的研究主要是围绕终端资源受限的设备，利用外包技术使得移动用户和PC端用户一样共享云端资源。2013 年 Li 等人[10]提出针对移动用户的低复杂性多机构 ABE，依赖移动用户与属性机构之间的半可信机构完成双方的信息交互；2014 年 Hohenberger 等人[11]提出了一种通过预计算降低 ABE 方案中加密运算计算量的方法——在线/离线外包 ABE 方案，将加/解密时的工作量分为在线和离线阶段分别完成，从而巧妙地提高用户应用体验。

以上研究工作为移动云环境安全的讨论提供了很好的过渡作用，直到近两年，面向移动云环境安全数据共享才被广泛探讨。2015 年，印度学者 Vijay 等人[12]提出针对属性撤销的移动云环境下的 CP-ABE 方案，该方案支持多属性机构同时工作；2016 年 Li 等人[13]提出了一个移动云环境下轻量级的数据共享方案，该方案通过改变访问控制树结构将大部分计算交给外部代理服务器，同时实现了撤销功能。以上这两个方案都需要一个中央权威机构，而中央权威机构完全可信不可保证。为减轻中央权威机构腐败带来的安全威胁，2017 年 Lyu 等人[14]提出无中心的移动云 ABE 方案，采用匿名密钥发布协议来实现隐私保护，此外利用在线/离线技术和外包解密可验证技术降低计算开销，同样实现了撤销功能；Zhao 等人[15]提出可验证外包计算的移动云 CP-ABE 方案，通过两种哈希函数对外包结果进行验证，但方案是针对单一授权机构的，无法解决现实应用场景中需要多机构授权管理用户的不同属性问题；De 等人[16]提出一种移动云环境下快速加、解密的 ABE 方案，可实现属性的分权；李学俊等人[17]采用双因子身份认证机制实现了对用户的匿名认证，提出一种移动云环境下无需 CA 的多机构 CP-ABE 方案。以上方案虽然在一定程度上解决了移动云环境下的数据共享问题，但都需要在系统运行前确定属性数量，并不能灵活添加属性而不用重置系统参数。

此外，针对云环境下的多机构场景问题，文献[19~22]提出了不同的解决方案。Yang 等人[18]提出了一个无中心的支持任意单调访问结构的可撤销方案；Huang 等人[19]提出的方案支持大属性域，可任意添加属性而不影响系统参数；Cui 等人[20]基于合数阶双线性群构造了一个可撤销方案；张凯等人[21]提出的无中心方案解密只需一个指数运算，且支持大属性域。然而以上方案均不同程度上存在用户端设备性能要求高、开销大，并不适合移动云环境。

安全方面考虑到自适应安全方案的设计(合数阶和素数阶)均需在一定程度上牺牲方案的性能，不适合移动云环境下的数据共享，而选择安全的方案又不能满足实际应用中对安全的需要。2015 年，Waters 团队的 Rouselakis 等人[22]提出了一种静态安全模型，以适应多授权机构的设置，将更符合多授权机构场景下的数据共享，在业界也有相当的认可度。相比于选择安全的方案和使用对偶系统加密技术证明满足自适应安全的方案，静态安全的方案具有令人满意的安全性和效率性。

就笔者所知，目前适用于移动云环境下的细粒度访问控制、高效且安全的多机构属性基加密问题还没有很好的解决方案：a)由于实际应用场景中，不同机构授权和管理用户的不同属性，由单一机构拓展为多授权机构的 ABE 方案计算量和管理复杂程度更高；b)目前提出的方案均是需要属性与机构在系统建立之初完成预设，后期增设还需要进行全局重置，实际效率仍不是非常理想；c)加密及解密阶段的计算量均与属性集合的大小或访问结构的规模成正比；d)安全性与效率性还有很大研究空间。本文提出一种无中心的 CP-ABE 方案，能有效应对多机构设置带来的计算量问题，且安全性能较已有方案有所提升，更适用于解决移动云环境的实际数据共享问题。

2　预备知识

本章主要对相关知识进行介绍。

2.1　双线性群

设 p 为素数，G 和 G_T 为 2 个 p 阶的循环群，g 是群 G 的生成元，$e:G^2 \to G_T$ 为一个映射，满足：

a)双线性。$\forall g,f \in G, a,b \in Z_N, e\left(g^a, f^b\right)=e\left(g,f\right)^{ab}$；

b)非退化。$\exists g \in G$ 使得 $e\left(g,g\right)$ 在群 G_T 中的阶为 p 。

假设群 G 和群 G_T 中的运算以及映射 e 均为多项式时间可计算的，并且在对群 G 和群 G_T 的描述中包含了每个群的一个生成元。

2.2 访问结构

令 $P=\{P_1,P_2,...,P_n\}$ 表示由 n 个参与方组成的集合，访问结构 A 是 P 的一个非空子集，即 $A\subseteq 2^P\setminus\{\varnothing\}$，其中，$2^P$ 表示 P 的所有子集组成的集合。若访问结构 A 是单调的，则 $\forall B,C$，若 $B\in A$ 且 $B\subseteq C$，那么 $C\in A$。在 A 中的集合称为授权集，不在 A 的集合称为非授权集。

2.3 线性秘密共享方案

一个关于参与者集合的秘密共享方案 Π 在 $\mathbb{Z}_p$ 上是线性的，则该方案满足以下两点：

a)所有参与者的分享份额构成 $\mathbb{Z}_p$ 上的一个向量。

b)存在 ℓ 行 n 列的矩阵 A，称做 Π 的分享生成矩阵，对于 $i=1,2,...,\ell$，函数 $\rho(i)$ 表示 A 第 i 行所标记的参与者。设列向量 $\boldsymbol{v}=(s,y_2,...,y_n)\in\mathbb{Z}_p$，其中：$s\in\mathbb{Z}_p$ 是需要共享的秘密；$y_2,...,y_n\in\mathbb{Z}_p$ 是随机选取的，则向量 $A\boldsymbol{v}$ 表示 Π 对秘密 s 的 ℓ 个分享份额，$(A\boldsymbol{v})_i$ 是第 i 个分享份额，它属于参与者 $\rho(i)$。

根据文献[23]对 LSSS 的定义，LSSS 具有线性重构特性。即若 Π 是一个关于访问结构的线性秘密共享方案，$S\in A$ 是一个授权集合，定义 $I\subseteq\{1,2,...,l\}$ 为 $I=\{i:\rho(i)\in S\}$，则可以在多项式时间内找到一组常数 $\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$，若 $\{\lambda_i\}$ 是对秘密 s 的有效分享，则等式 $\sum_{i\in I}\omega_i\lambda_i=s$ 成立，而对非授权集合是不存在这样的常数的。

2.4 复杂性假设

q-DBPBDHE2 假设[22]。群 G 中 q-DBPBDHE2 问题叙述如下：随机选取 $a,s,b_1,b_2,...,b_q\in\mathbb{Z}_p^*$，已知

$$D=\begin{pmatrix} p,g,G,e,g^s,\{g^{a^i}\}_{i\in[2q],i\neq q+1},\{g^{b_j a^i}\}_{(i,j)\in[2q,q],i\neq q+1}, \\ \{g^{s/b_i}\}_{i\in[q]},\{g^{sa^i b_j/b_{j'}}\}_{(i,j,j')\in[q+1,q,q],j\neq j'} \end{pmatrix},$$

区分 $e(g,g)^{sa^{q+1}}$ 和 G_T 中的随机元素 R。当

$$\left|\Pr\left[\beta\left(D,e(g,g)^{sa^{q+1}}\right)=0\right]-\Pr\left[\beta\left(D,R\right)=0\right]\right|\geq\varepsilon,$$

则称算法 β 以 ε 的优势解决 q-DBPBDHE2 问题。

若任何多项式时间算法攻破 q-DBPBDHE2 问题的优势 ε 都是可忽略的，则称 q-DBPBDHE2 假设在群 G 中成立。

3 方案与安全模型

针对移动云计算在数据安全共享方面存在的问题，基于属性基加密方法设计一种移动云环境下的高效数据安全共享架构，提出更贴近实际应用场景、满足用户细粒度访问控制，确保用户在数据共享时获得更好的用户体验，实现移动云环境下数据安全、受控、灵活、高效地共享。

3.1 共享框架

该方案主要包括四个实体，分别是数据拥有者 DO(data owner)、移动用户 DU(data user)、多个属性权威机构 AA(attribute authority)、云服务提供商 CSP(cloud server provider)。共享框架如图 1 所示。

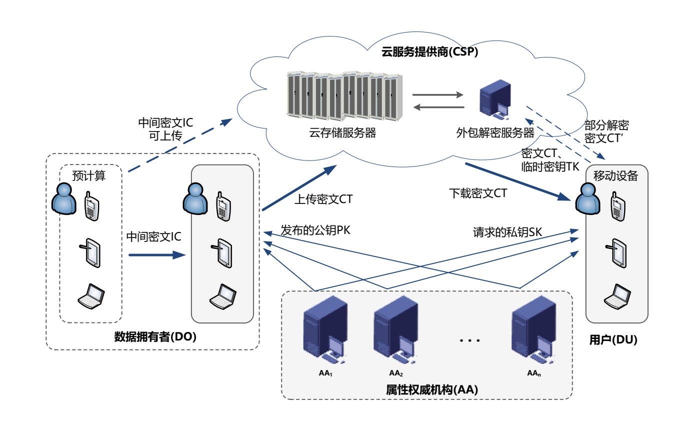


图 1　共享框架

1)数据拥有者 DO

DO 主要是按照安全策略拟定访问结构，然后通过预计算根据访问结构完成数据加密，最后将加密结果，即与访问策略相关联的密文上传至云端。

2)终端用户 DU

任何用户都可以自由访问并获取云服务器上的密文文件，当且仅当 DU 拥有的属性满足密文的访问策略时才能解密。用户拥有的属性是由多个属性权威机构根据用户的权限进行分发，以此来实现密文的跨域访问。

3) 多权威机构 AA

AA 向用户进行授权，产生公、私钥对，发布其公钥并秘密保存私钥。本文假设方案中的每一个属性都是由一个特定的 AA 授权(如身份证号由派出所授权，而硕士学位由学校授权)，而每个 AA 都可以管理多个属性(如研究生学位处可授权硕士学位和博士学位等)。在实践中，可以将属性看做是 AA 的公钥和一个属性的组合，这将确保当有多个 AA 属性重复时，则与系统中的不同属性相对应(如清华大学的硕士研究生和北京大学的硕士研究生)。

4)云服务提供商 CSP

笔者认为云服务提供商拥有强大的存储和计算能力，DU 无须过多考虑自身的硬件和软件条件，可通过不同配置的设备访问 CSP 以获取其授权资源。其次，CSP 一般被看做是诚实且好奇的，为此，CSP 只被用于存储密文和进行部分解密，不能从中获取关于数据或密钥的任何信息。

这里的 DO、DU 主要指的是低端设备用户，如手机、车载系统等，也可以是 PC 机等高端设备用户，在此不再赘述。

3.2 方案的形式化定义

定义属性空间 U，权威机构空间 V，函数 $T:U\rightarrow V$ 是属性空间到权威机构空间的一个满射，即 $i\in U$，$T(i)\in V$。另外，方案中的每个用户(AA 也可看做是特殊的用户)都拥有唯一的

全局标志符 GID 和一个由多个 AA 授权的属性集合 S 。

一个适用于移动云环境下的多机构密文策略属性基加密方案主要由下面的八个算法描述:

a) 全局初始化算法 $\text{GlobalSetup}(\lambda) \to \text{GP}$ 。

λ 为安全参数，经过初始化输出全局的公共参数 GP 。GP 作为剩余七种算法的公共输入参数。为简明扼要，以下算法将不再提及。

b) 各权威机构初始化算法(各权威机构注册算法) $\text{AuthoritySetup}(\text{GID}_\beta) \to \{\text{PK}_\beta, \text{SK}_\beta\}$ 。

由各权威机构独立运行，输入 $\text{GID}_\beta(\beta \in V)$ 输出各权威机构的公、私钥对 $\{\text{PK}_\beta, \text{SK}_\beta\}$ 。

c) 用户注册算法 $\text{KeyGen}_{\text{user}}(\text{GID}_i) \to \{\text{userPK}_i, \text{key}\}$ 。

即经典方案中密钥生成算法的用户部分，由用户完成，输入 $\text{GID}_i (i \in U)$ ，输出用户的公、私钥对 $\{\text{userPK}_i, \text{key}\}$ 。

d) 云服务提供商 CSP 外包解密服务器密钥生成算法 $\text{KeyGen}_{\text{out}}(\text{GID}_i, \text{userPK}_i, S, \{\text{SK}_j\}) \to \text{SK}_{\text{out}}$ 。

即经典方案中密钥生成算法的外包部分，由用户运行。如用户 i ，输入标志 GID_i 、公钥 userPK_i 、用户属性集 S 和相关权威机构(即 $\forall i \in S, T(i) = \beta$)的私钥集 $\{\text{SK}_\beta\}$ ，输出针对用户 i 的外包解密密钥 SK_{out} ，秘密上传至云存储服务器。

e) 预计算算法 $\text{Pre}_{\text{enc}}(\{\text{PK}_\beta\}) \to \text{IC}$ 。

由用户在设备空闲时运行，根据用户定义的访问策略输入相关属性权威机构的公钥集 $\{\text{PK}_\beta\}$ ，输出临时密文 IC ，可上传至云存储服务器。

f)加密算法 $\text{Encrypt}(\text{IC}, M, (A, \rho)) \to \text{CT}$ 。

输入临时密文 IC ，待加密的明文 M ，由用户定义的访问结构 (A, ρ) ，输出密文 CT ，并上传至云存储服务器（此算法也可跳过预计算操作直接对明文进行加密）。

g) 外包解密算法 $\text{Out}_{\text{dec}}(\text{SK}_{\text{out}}, \text{userPK}_i, \text{CT}) \to \text{CT}'$ 。

由 CSP 的外包解密服务器运行，输入用户 i 的外包解密密钥 SK_{out} ，公钥 userPK_i 和密文 CT 。当 SK_{out} 中关联的属性集 S 不满足密文 CT 中的访问策略 (A, ρ) 时，解密失败；否则输出半解密密文 CT' ，将其发送给用户 i 。

h) 终端解密算法 $\text{Decrypt}(\text{key}, \text{CT}') \to M$ 。

由授权用户设备运行，输入用户私钥 key 和半解密密文 CT' ，输出明文 M 。

3.3 安全模型

本文定义的静态安全模型是挑战者与攻击者之间的一个安全游戏，它与自适应模型的区别在于攻击者必须在收到公共参数后立即指定攻击对象和询问内容，然后发送给挑战者，并且在游戏结束后才能改变。与自适应模型相同的是，静态安全模型还允许攻击者可以多次对用户私钥和云端存储的部分解密密文进行询问，也就是说攻击者可以通过询问外包解密密钥来解密密文，从而得到部分解密密文。此外，还允许攻击者通过腐化部分权威机构从而生成权威机构的公钥参与加密。模型修改自文献[22]，主要是在抵抗云服务器攻击基础上通过对私钥的询问增加了抵抗多个合法用户的合谋攻击，可通过下面几个阶段的游戏进行描述：

a)创建设置。挑战者运行方案中的全局初始化算法，并将公共参数 GP 发送给攻击者。

b)询问。攻击者首先从权威机构 V 中选择被腐化的一部分机构 C ($C \subseteq V$)生成并发送其公钥 $\{\text{PK}_\beta\}_{\beta \in C}$ 给挑战者，接着向挑战者询问如下：

(a)选取 m 个授权用户 $\{\text{GID}_i\}_{i=1}^m$ ，询问其公、私钥。

(b)选取部分未被腐化的权威机构 N ($N \subseteq V$)，询问其公钥。

(c)选取 n 个用户 $\{S_i, \text{GID}_i\}_{i=1}^n$ ，询问其外包解密密钥。其中，$S_i \subseteq U$ 为用户 i 拥有的属性集，要求 $T(S_i) \cap C = \varnothing$ ，即用户拥有的属性都是由未被腐化的权威机构授权的。此外，要求 $n > m$ ，即攻击者不仅能够询问 a)中用户的外包解密密钥，也能够询问其他用户对应的外包解密密钥。

(d)选取 2 个等长的消息 m_0, m_1 和一个访问策略 (A, ρ) ，询问其挑战密文。其中，要求对每个询问过私钥的用户 $i (1 \le i \le n)$ 的属性集 $S_i \cup S_C$ 都不能满足访问策略 (A, ρ) 。

c)挑战者应答。挑战者随机选择 $b \in \{0,1\}$ ，返回

(a)用户 $\{\text{GID}_i\}_{i=1}^m$ 的公、私钥 $\{\text{userPK}_{\text{GID}_i}, \text{key}\}_{i=1}^m$ 。

(b)授权机构 $N \subseteq V$ 的公钥 $\{\text{PK}_\beta\}_{\beta \in N}$ 。

(c)外包解密密钥 $\{\text{SK}_{\text{out}}\}_{i=1}^n$ 。

(d)挑战密文 CT* 。

d)猜测。攻击者输出猜测结果 $b' \in \{0,1\}$ 。定义攻击者赢得该游戏的优势为 $\left|\Pr[b = b'] - \frac{1}{2}\right|$ 。

定 义 若攻击者赢得该游戏的优势不可忽略，则称该方案是静态安全的。

上述游戏中不包含 a)类询问时，此安全模型转换为只针对云服务器攻击。

4 具体方案

本文提出的方案借鉴了文献[21]的映射思想，利用函数 T 将属性 $i \in U$ 映射到授权 i 的权威机构 $\beta \in V$ ，即存在满射 $\delta(x)$ 可将矩阵的行和一个权威机构对应起来，有 $\delta(x) = T(\rho(x)) \to \beta$ 。此外，在方案加密前引入了预计算的外包操作，并将移动云属性基安全共享划分为四个方面，即初始化、用户注册、数据加密、数据访问。具体构造如下：

a)初始化。

首先执行 GlobalSetup 算法，产生全局的公共参数 GP 。选择一个素数阶双线性群 G ， p 为阶数， g 为生成元。然后选择两个哈希函数 H 和 F ， $H: \mathbb{Z}_p^* \to G$ ，将用户标志符 GID 映射到 G 中， $F: U \to G$ ，将属性映射到 G 中。输出全局公共参数 $\text{GP} = \{p, G, g, H, F, U, V, T\}$

由每个权威机构 $\beta \in V$ 运行算法 AuthoritySetup ，随机选取

$\alpha_\beta, y_\beta \in \mathbb{Z}_p^*$，公开自己的公钥 $\mathrm{PK}_\beta = \{e(g,g)^{\alpha_\beta}, g^{y_\beta}\}$，秘密保留自己的私钥 $\mathrm{SK}_\beta = \{\alpha_\beta, y_\beta\}$。

b)用户注册。

当新用户访问系统时，用户需要向属性授权机构请求私钥。私钥由用户属性集 S 中的每个属性对应的权威机构通过执行 $\mathrm{KeyGen_{out}}$ 算法联合生成。首先，在移动设备上运行 $\mathrm{KeyGen_{user}}$ 算法，随机选择 $z \in \mathbb{Z}_p^*$，利用自身的 GID_i 计算生成用户公钥 $\mathrm{userPK_{GID_i}} = \{g^z, H(\mathrm{GID}_i)^z\}$ 并将其公布。相关权威机构利用 $\mathrm{userPK_{GID_i}}$ 输出针对用户 GID_i 的外包解密密钥 $\mathrm{SK_{out}}$，从而加入基于属性的数据共享系统。

具体为对于用户属性集 S 中的每一个属性 i，如果 $T(i)=\beta$，则授权机构 β 选择随机元 $t_i \in \mathbb{Z}_p^*$，并计算：

$$K_{i,1} = g^{z\alpha_i} H(\mathrm{GID})^{zy_i} F(i)^{t_i},$$

$$K_{i,2} = g^{t_i},$$

输出密钥 $\mathrm{SK}_S = \{S, K_{i,1}, K_{i,2}\}_{i\in S}$。

用户将私钥 $\mathrm{key} = 1/z$ 秘密保存，并计算：

$$K'_{i,1} = K_{i,1}^{1/z},$$

$$K'_{i,2} = K_{i,2}^{1/z},$$

输出云服务器解密密钥：

$$\mathrm{SK_{out}} = \{S, K'_{i,1}, K'_{i,2}\}_{i\in S},$$

将 $\{\mathrm{GID}, \mathrm{SK_{out}}\}$ 加入云服务器密钥列表 Klist 中。

c)数据加密。

当移动设备空闲时，运行 $\mathrm{Pre_{enc}}$ 算法，主要是在正式加密之前，对 U 中的每个属性 i 都先完成预计算，为之后的加密提供计算结果。即对属性 i，随机选择 $\lambda'_i, \omega'_i, r_i \in \mathbb{Z}_p^*$，并计算：

$$\mathrm{IC}_{i,1} = \mathrm{e}(g,g)^{\lambda'_i} e(g,g)^{\alpha_i r_i},$$

$$\mathrm{IC}_{i,2} = g^{-r_i},$$

$$\mathrm{IC}_{i,3} = g^{y_i r_i} g^{\omega'_i},$$

$$\mathrm{IC}_{i,4} = F(i)^{r_i}$$

中间密文 $\mathrm{IC} = \{\mathrm{IC}_{i,1}, \mathrm{IC}_{i,2}, \mathrm{IC}_{i,3}, \mathrm{IC}_{i,4}\}_{i\in U}$，加密者可以选择将其上传至 CSP 的外包存储服务器来节省设备的存储资源。

临时密钥 $\mathrm{TK} = \{\lambda'_i, \omega'_i\}_{i\in U}$ 保存在本地。

当移动用户需要进行秘密数据共享时，运行 Encrypt 算法，依次输入消息 m，访问策略 (A,ρ)，以及中间密文 IC 和临时密钥 TK。而后随机选择 $s, y_2, \ldots, y_n, z_2, \ldots, z_n \in \mathbb{Z}_p^*$，令向量 $\boldsymbol{v} = (s, y_2, \ldots, y_n)^T$，$\boldsymbol{\omega} = (0, z_2, \ldots, z_n)^T$，对于所有的 $x \in [\ell]$，计算 $\lambda_x = (A\boldsymbol{v})_x$，$\omega_x = (A\boldsymbol{\omega})_x$。有 $\delta(x) = T(\rho(x)) \to \beta$，可将 $x \in [\ell]$ 映射到权威机构 β。计算密文：

$$C_0 = me(g,g)^s,$$

$$C_{x,j} = \mathrm{IC}_{\rho(x),j} \big| j \in \{\mathbb{Z}_p^* | 1 \le j \le 4\},$$

$$C_{x,5} = \lambda_x - \lambda'_{\rho(x)},$$

$$C_{x,6} = \omega_x - \omega'_{\rho(x)},$$

输出密文 $\mathrm{CT} = ((A,\rho), C_0, \{C_{x,j}\}_{x\in[\ell], j\in\{\mathbb{Z}_p^*|1\le j\le 6\}})$。

以上运算也可由数据拥有者在正式加密时按需要只对相关属性进行预计算，再完成加密，此处设计借鉴了在线\离线思想，充分利用了用户端的空闲时间和云存储的能力，为正式加密阶段提供部分计算结果，一定程度上缓解加密压力。

d)数据访问。

DU 从 CSP 下载密文。如果密文是合法的，那么移动端使用私钥完成解密。

云服务器在接到访问请求时，首先根据终端用户公钥 $\mathrm{userPK_{GID}}$ 在云服务器密钥列表 Klist 中查找其相对应的云服务器解密密钥 $\mathrm{SK_{out}} = \{S, K'_{i,1}, K'_{i,2}\}_{i\in S}$，然后运行 $\mathrm{Out_{dec}}$ 算法对密文 $\mathrm{CT} = ((A,\rho), C_0, \{C_{x,j}\}_{x\in[\ell], j\in\{\mathbb{Z}_p^*|1\le j\le 6\}})$ 进行部分解密。当终端用户在外包解密服务器的密钥中关联的属性集合 S 不满足密文中的访问策略 (A,ρ) 时，则解密失败；否则令 $I = \{x : \rho(x) \in S\} \subseteq \{1,2,\ldots,\ell\}$，解密服务器计算 $\{c_x \in Z_p\}$ 满足 $\sum_{x\in I} c_x A_x = (1,0,\ldots,0)$，最后将部分解密的密文 $\mathrm{CT}' = (C_0, C_{\mathrm{part1}}, C_{\mathrm{part2}})$ 发送给 DU。其中：

$$C_{\mathrm{part1}} = \prod_{x\in I} \{C_{x,1} \cdot e(g,g)^{C_{x,5}} e(K'_{\delta(x),1}, C_{x,2}) e(K'_{\delta(x),2}, C_{x,4})\}^{c_x}$$

$$C_{\mathrm{part2}} = \prod_{x\in I} \{e(H(\mathrm{GID})^z, C_{x,3} \cdot g^{C_{x,6}})\}^{c_x}$$

终端用户在收到云服务器部分解密的密文后，运行 Decrypt 算法，利用保留的用户私钥 $\mathrm{key} = 1/z$ 完成剩余解密运算，计算 $C_{\mathrm{part1}} \cdot C_{\mathrm{part2}}{}^{1/z} = e(g,g)^s$，最后恢复：

$$m = \frac{C_0}{C_{\mathrm{part1}} \cdot C_{\mathrm{part2}}{}^{1/z}}$$

5 方案分析

5.1 正确性分析

a)外包解密过程。当属性集 S 满足访问策略 (A,ρ)，令 $I = \{x : \rho(x) \in S\} \subseteq \{1,2,\ldots,\ell\}$，则常数 $\{c_x \in \mathbb{Z}_p\}$ 满足 $\sum_{x\in I} \lambda_x c_x = s$ 和 $\sum_{x\in I} \omega_x c_x = 0$。有如下结果：

$$C_{\mathrm{part1}} = \prod_{x\in I} \{C_{x,1} \cdot e(g,g)^{C_{x,5}} e(K'_{\delta(x),1}, C_{x,2}) e(K'_{\delta(x),2}, C_{x,4})\}^{c_x}$$

$$=\prod_{x\in I}\{e(g,g)^{\lambda'_{\rho(x)}}e(g,g)^{\alpha_{\rho(x)}r_{\rho(x)}}e(g,g)^{(\lambda_x-\lambda'_{\rho(x)})}e((g^{z\alpha_{\rho(x)}}H(\mathrm{GID})^{zy_{\rho(x)}}F(\rho(x))^{t_{\rho(x)}})^{1/z},g^{-r_{\rho(x)}})e((g^{t_{\rho(x)}})^{1/z},F(\rho(x))^{r_{\rho(x)}})\}^{c_x}$$

$$=\prod_{x\in I}\{e(g,g)^{\alpha_{\rho(x)}r_{\rho(x)}}e(g,g)^{\lambda_x}e((g,g)^{-\alpha_{\rho(x)}r_{\rho(x)}}e(H(\mathrm{GID}),g)^{-y_{\rho(x)}r_{\rho(x)}}e(F(\rho(x)),g)^{-r_{\rho(x)}t_{\rho(x)}/z}e((g,F(\rho(x)))^{r_{\rho(x)}t_{\rho(x)}/z}\}^{c_x}$$

$$=\prod_{x\in I}\{e(g,g)^{\lambda_x}e(H(\mathrm{GID}),g)^{-y_{\rho(x)}r_{\rho(x)}}\}^{c_x}$$

$$=e(g,g)^{\sum_{x\in I}\lambda_x c_x}e(H(\mathrm{GID}),g)^{-\sum_{x\in I}y_{\rho(x)}r_{\rho(x)}c_x}$$

$$=e(g,g)^{s}e(H(\mathrm{GID}),g)^{-\sum_{x\in I}y_{\rho(x)}r_{\rho(x)}c_x}$$

$$C_{\mathrm{part}2}$$

$$=\prod_{x\in I}\{e(H(\mathrm{GID})^{z},C_{x,3}\cdot g^{C_{x,6}})\}^{c_x}$$

$$=\prod_{x\in I}\{e(H(\mathrm{GID})^{z},g^{y_{\rho(x)}r_{\rho(x)}}g^{\omega'_{\rho(x)}}\cdot g^{(\omega_x-\omega'_{\rho(x)})})\}^{c_x}$$

$$=\prod_{x\in I}\{e(H(\mathrm{GID})^{z},g^{y_{\rho(x)}r_{\rho(x)}}g^{\omega_x})\}^{c_x}$$

$$=\prod_{x\in I}\{e(H(\mathrm{GID}),g)^{z\cdot y_{\rho(x)}r_{\rho(x)}}e(H(\mathrm{GID}),g)^{z\cdot\omega_x}\}^{c_x}$$

$$=e(H(\mathrm{GID}),g)^{z\sum_{x\in I}y_{\rho(x)}r_{\rho(x)}c_x}e(H(\mathrm{GID}),g)^{z\sum_{x\in I}\omega_x c_x}$$

$$=e(H(\mathrm{GID}),g)^{z\sum_{x\in I}y_{\rho(x)}r_{\rho(x)}c_x}$$

b)移动设备完成最终解密。

$$C_{\mathrm{part}1}\cdot C_{\mathrm{part}2}{}^{1/z}$$
$$=\{e(g,g)^{s}e(H(\mathrm{GID}),g)^{-\sum_{x\in I}y_{\rho(x)}r_{\rho(x)}c_x}\}(e(H(\mathrm{GID}),g)^{z\sum_{x\in I}y_{\rho(x)}r_{\rho(x)}c_x})^{1/z}$$
$$=e(g,g)^{s}$$

$$\frac{C_0}{C_{\mathrm{part}1}\cdot C_{\mathrm{part}2}{}^{1/z}}=\frac{me(g,g)^{s}}{e(g,g)^{s}}=m$$

5.2 安全性分析

引理 1 假定 Rouselakis-Waters(RW)方案[22]是静态安全的，则本文提出的移动云环境下无中心多机构 CP-ABE 方案也是静态安全的。

证 明 假设攻击者以概率多项式时间攻破本方案的优势不可忽略，那么就可以构造一个概率多项式时间的算法 Φ 来破 RW 方案。

Φ 运行 GlobalSetup 算法，输出全局公共参数 $\mathrm{GP}=\{p,G,g,H,F,U,V,T\}$，并将其发送给攻击者。

1)询问　攻击者首先从权威机构 V 中选择被腐化的一部分机构 C ($C\subseteq V$)生成并发送其公钥 $\{\mathrm{PK}_\beta\}_{\beta\in C}$ 给模拟者 Φ，接着向模拟者询问如下：

a)选取 m 个授权用户 $\{\mathrm{GID}_i\}_{i=1}^{m}$，询问其公、私钥。

b)选取部分未被腐化的权威机构 N ($N\subseteq V$)，询问其公钥。

c)选取 n 个用户 $\{S_i,\mathrm{GID}_i\}_{i=1}^{n}$，询问其外包解密密钥。其中，$S_i\subseteq U$ 为用户 i 拥有的属性集，要求 $T(S_i)\cap C=\varnothing$，即用户拥有的属性都是由未被腐化的权威机构授权的。此外，要求 $n>m$，即攻击者不仅能够询问 a)中用户的外包解密密钥，也能够询问其他用户对应的外包解密密钥。

d)选取两个等长的消息 m_0,m_1 和一个访问策略 (A,ρ)，询问其挑战密文。其中，要求对每个询问过私钥的用户 $i(1\le i\le n)$ 的属性集 $S_i\cup S_C$ 都不能满足访问策略 (A,ρ)。

2)挑战者应答　模拟者 Φ 给挑战者发送公钥 $\{\mathrm{PK}_\beta\}_{\beta\in C}$，并询问 RW 方案中 $N\subseteq V$ 对应的公钥，$\{S_i,\mathrm{GID}_i\}_{i=1}^{m}$ 对应的私钥和挑战密文。挑战者给 Φ 返回相应的私钥 $\{\mathrm{SK}_{S_i,\mathrm{GID}_i}=(g^{\alpha_\beta}H(\mathrm{GID}_i)^{y_\beta}F(j)^{t_j},g^{t_j})_{j\in S_i}\}_{i=1}^{m}$、公钥 $\{\mathrm{PK}_\beta\}_{\beta\in N}$ 和挑战密文 CT*。Φ 首先计算本方案中的用户私钥：对 $1\le i\le m$，随机选取 $z\in\mathbb{Z}_p^*$，计算用户公钥 $\mathrm{userPK}_{\mathrm{GID}_i}=\{g^{z},H(\mathrm{GID}_i)^{z}\}$ 和私钥 $\mathrm{key}_{\mathrm{GID}_i}=\{1/z\}_i$，然后计算 $\{S_i,\mathrm{GID}_i\}_{i=1}^{n}$ 对应的外包解密密钥，如下所示:

a)对 $1\le i\le m$， $j\in S_i$，计算

$$K_{j,1,\mathrm{GID}_i}=(g^{\alpha_\beta}H(\mathrm{GID}_i)^{y_\beta}F(j)^{t_j})^{z_i}=g^{\alpha_\beta z_i}H(\mathrm{GID}_i)^{y_\beta z_i}F(j)^{t_j z_i},$$

$$K_{j,2,\mathrm{GID}_i}=(F(j)^{t_j})^{z_i}=F(j)^{t_j z_i},$$

令 $\mathrm{SK}_{\mathrm{out,GID}_i}=\{S_i,K_{i,1,\mathrm{GID}_i}{}^{z_i},K_{i,2,\mathrm{GID}_i}{}^{z_i}\}_{j\in S_i}$

b)对 $m\le i\le n$， $j\in S_i$，随机选取 $g_j\in G$ 和 $k_j\in\mathbb{Z}_p^*$，计算 $K_{j,1,\mathrm{GID}_i}=g_jF(j)^{k_j}g_j$， $K_{j,2,\mathrm{GID}_i}=F(j)^{k_j}$。令 $\mathrm{SK}_{\mathrm{out,GID}_i}=\{S_i,K_{i,1,\mathrm{GID}_i}{}^{z_i},K_{i,2,\mathrm{GID}_i}{}^{z_i}\}_{j\in S_i}$。注意 $g^{\alpha_\beta}H(\mathrm{GID}_i)^{y_\beta}$ 是群 G 中的元素，而 G 是循环群，所以存在未知的 $z_i\in\mathbb{Z}_p^*$ 使

$$g_j=(g^{\alpha_\beta}H(\mathrm{GID}_i)^{y_\beta})^{z_i}=g^{\alpha_\beta z_i}H(\mathrm{GID}_i)^{y_\beta z_i}$$

因此，

$$K_{j,1,\mathrm{GID}_i}=g_jF(j)^{k_j}=g^{\alpha_\beta z_i}H(\mathrm{GID}_i)^{y_\beta z_i}F(j)^{k_j}$$

$$K_{j,2,\mathrm{GID}_i}=F(j)^{k_j}$$

是合理分布的外包解密密钥。

Φ 将上述用户公、私钥 $\{\mathrm{userPK}_{\mathrm{GID}_i},\mathrm{key}\}_{i=1}^{m}$、权威机构公钥 $\{\mathrm{PK}_\beta\}_{\beta\in N}$、外包解密密钥 $\{\mathrm{SK}_{\mathrm{out,GID}_i}\}_{i=m}^{n}$ 和挑战密文 CT* 发送给攻击者。

3)猜测　攻击者和 Φ 同时输出猜测结果 $b'\in\{0,1\}$。

上述分布对攻击者来说是真实不可区分的，因此，若攻击

者能以不可忽略的优势攻破本方案，则也能以不可忽略的优势攻破 RW 方案。

引理 2 假定 q-DPBDHE2 假设成立，则 RW 方案在随机预言模型下是静态安全的。

证 明 文献[22]已给出详细的证明，由于篇幅原因，在此不再赘述。

定理 1 假定 q-DPBDHE2 假设成立，则本文的方案在随机预言模型下是静态安全的。

证 明 由引理 1 和 2 直接得证。

5.3 效能分析

本节主要对本方案和相关方案的效能进行了对比分析，包括方案本身功能性的实现和用户端的开销(存储开销和计算开销)。表 1 给出了方案的功能性对比结果，表 2 给出了方案的开销对比结果。

表 1 功能对比

	无 CA	大属性域	素数阶	预计算	外包解密
文献[18]	×	×	√	×	×
文献[19]	×	√	√	×	√
文献[20]	√	×	×	×	×
文献[21]	√	√	√	×	√
本方案	√	√	√	√	√

本文主要考虑更符合实际应用中的多权威机构设置，因此选择了四个多权威机构的相近方案与本方案做比对。文献[18,19]给出的方案都需要一个中央权威机构对身份进行认证，不能避免中央机构腐败对整个加密过程带来的威胁，且中央权威机构必须要与每个权威机构进行信息的交互，由此带来的通信开销也不能忽视；文献[20]考虑了以上的问题，但方案是基于合数阶双线性群提出的，在效率上与素数阶的方案相差较大，且并未考虑其他降低开销的办法；相比之下，文献[21]提出了一个比较好的解决方案，但对于移动云用户来说在加密阶段的开销仍然要求较高。本文提出的方案在总结前人研究成果的基础上，对以上涉及到的不足进行了改进，在加密阶段引入了预计算操作，使得用户可以充分利用设备的空闲时间和云存储空间，在不泄漏任何秘密信息的前提下，为正式加密提供部分计算结果参与加密，使其更适用于移动云环境。

此外，本文提出的方案借鉴了文献[21]的映射思想，采用函数 $F:U\to G$，将属性空间映射到 G 中，这样的好处是系统中的属性个数不用限制，任何 G 中的字符串都可以在后期作为一个新的属性添加到方案中。此外，本方案通过函数 H 将用户标志符 GID 映射到 G 中，使得拥有唯一标志的用户和机构都可以实现完全分权，以此抵抗用户和机构间的合谋攻击。

表 2 开销对比

	公钥	用户私钥	用户端加密	用户端解密
文献[18]	$2\|U\|+3$	$\|S\|+2$	$(5\ell+3)E$	$2\|I\|P+\|I\|E$
文献[19]	4	$2\|S\|+2$	$(2\ell+2)E$	$(2\|I\|+2)P+\|I\|E$
文献[20]	$2\|U\|$	$\|S\|$	$(5\ell+1)E$	$2\|I\|P+\|I\|E$
文献[21]	$2\|V\|$	1	$(6\ell+1)E$	E
本方案	$2\|V\|$	1	E	E

本文对比了方案的存储开销和计算开销，如表 2 所示。其中 $|U|$ 表示属性个数，$|V|$ 表示权威机构个数，$|S|$ 表示用户的属性个数，ℓ 表示访问结构中矩阵的行数，$|I|(|I|\le\ell)$ 表示参与解密的矩阵行数，P 表示群中双线性对运算，E 表示群中的指数运算。由于乘法运算与群中双线性运算和指数运算的开销相比大可忽略不计，在此处只考虑了以上运算的开销。

从表中可以看出，在 AA 公钥方面，文献[19]可达常数，但其方案需要存在一个中央权威机构，而中央权威机构的私钥是与 $|V|$ 线性相关的。由于本文方案采用函数 T 将属性 $i\in U$ 映射到授权 i 的权威机构 $j\in V$，所以 $|V|\le|U|$，也就是说本方案中 AA 公钥只与属性的授权机构的个数有关，而与所管理的属性个数无关。这样的好处是在后期加入属性也不会影响 AA 的公钥。所以本方案在用户存储开销上是优于文献[18]和[20]的。

其次，在用户的私钥方面，文献[18~20]中 AA 根据用户的属性直接生成，因此私钥长度与 $|S|$ 线性相关。本文方案是先让用户在注册阶段就为自己产生一组公、私钥对，然后 AA 再利用这组公、私钥对和用户的属性为云服务器产生外包解密密钥。这样用户端的私钥即为常数，而不会随着用户属性的增长而增大。因此，本文方案的用户端存储开销是小于文献[18~20]提出的方案的。

在计算开销方面，由于本文主要研究的是适用于数据共享的 CP-ABE 方案，访问策略是与密文相关联的，即密文的长度和访问策略中访问矩阵的行数 ℓ 线性相关。本文方案在加密和解密时都考虑了外包的情形，因此在加、解密的效率上要优于文献[18~20]。在保证安全的前提下，在用户端的加密时采用在线/离线思想，在用户设备空闲时，即离线阶段执行一部份计算，使得在线加密量明显降低，达到一次双线性运算和一次指数运算，因此本文方案要在加密时要优于文献[21]。

用户端解密时，文献[18~20]是用户直接对密文进行解密，因此解密时的双线性对运算与指数运算都是与 $|I|$ 线性相关的。而本文方案是由云外包解密服务器先进行部分解密，最后用户只需要对中间密文进行一次指数运算就可以恢复出明文，大大降低了端设备的计算开销，适用于移动云中的秘密共享。

5.4 实验结果

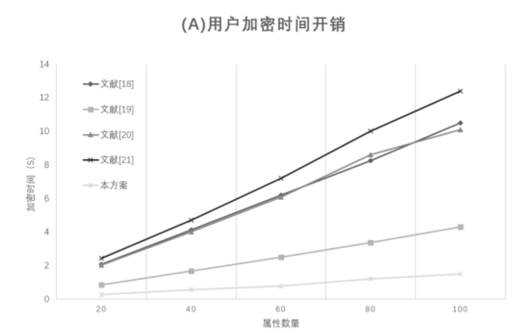
本节通过实验综合对比了本文方案与相关文献的计算开销。实验环境为 Intel Core i7，2.6 GHz，8 GB 内存，操作系统为 Linux MINT 18，基于 Charm 架构[24]，选用 JPBC 中的 D 类椭圆曲线。实验中，在比较用户端的加、解密效率可以看出，本文方案比文献[21]在加密效率上有更大优势。

实验结果如图 2 所示。计算开销方面本文方案更胜一筹，适用于云环境下资源受限的用户进行数据安全共享。

6 结束语

本文方案在经典 ABE 方案的基础上，一是在加密时采取了

预计算方法、解密时进行了安全外包，有效降低了加、解密时用户端的计算开销；二是引入了映射思想，在方案构建之初，将属性与群元素进行一一对映，以满足后续随时添加属性而不会影响整体方案运行的需要；三是考虑了更加符合实际应用的无中心多权威机构情景，权威机构与用户拥有唯一身份标识，各自独立运行分发保管密钥，属性由唯一权威机构授权，但可由多个权威机构管理；最后在随机预言模型下对本文方案的安全性进行了证明。方案分析和实验结果表明，本文方案可以有效减少移动设备端的开销，适用于移动云环境下的数据安全共享。



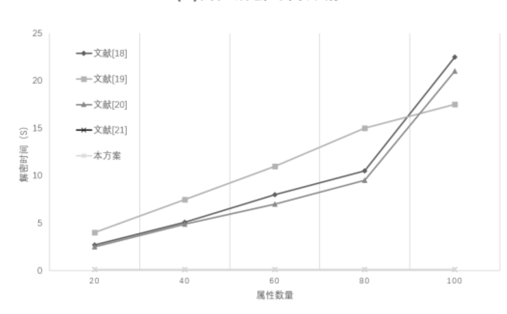


图 2　加、解密时间开销

参考文献：

[1] Mell P, Grance T. The NIST definition of cloud computing [J]. Communications of the ACM, 2011, 53 (6): 50-50.

[2] White Paper. Mobile cloud computing solution brief [R]. 2010.

[3] 崔勇，宋健，缪葱葱，等．移动云计算研究进展与趋势 [J]. 计算机学报, 2017, 40 (2): 273-295. (Cui Yong, Song Jian, Miao Congcong, *et al.* Mobile cloud computing research progress and trends [J]. Chinese Journal of Computers, 2017, 40 (2): 273-295.)

[4] Gartner. Five trends in cybersecurity for 2017 and 2018 [EB/OL]. https://www. gartner. com/smarterwithgartner/5-trends-in-cybersecurity-for-2017-and-2018/.

[5] Wikipedia. The definition of mobile cloud computing [EB/OL]. https://en. wikipedia. org/wiki/Mobile_cloud_computing.

[6] 苏航，朱智强，孙磊．适合移动云存储的基于属性的关键词搜索加密方案 [J]. 计算机研究与发展, 2017, 54 (10): 2369-2377. (Su Hang, Zhu Zhiqiang, Sun Lei. Attribute-based encryption with keyword search in mobile cloud storage [J]. Journal of Computer Research and Development, 2017, 54 (10): 2369-2377.)

[7] 曹磊．移动医疗中隐藏访问结构的云外包属性基加密 [D]. 西安：西安电子科技大学, 2015. (Cao Lei. Outsourcing the attribute-based encryption for mobile medical data hiding access structure [D]. Xi’an: Xidian university, 2015.)

[8] Khan A N, Kiah M L M, Khan S U, *et al.* Towards secure mobile cloud computing: a survey [J]. Future Generation Computer Systems, 2013, 29 (5): 1278-1299.

[9] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts [C]// Proc of Usenix Conference on Security. [S. l.] : USENIX Association, 2011: 34-34.

[10] Li Fei, Rahulamathavan Y, Rajarajan M, *et al.* Low complexity multi-authority attribute based encryption scheme for mobile cloud computing [C]// Proc of IEEE, International Symposium on Service Oriented System Engineering. 2013: 573-577.

[11] Hohenberger S, Waters B. Online//offline attribute-based encryption [M]// Public-Key Cryptography-PKC 2014. Berlin: Springer, 2014: 293–310.

[12] Vijay H, Goyal D, Singla S. An efficient and secure solution for attribute revocation problem utilizing CP-ABE scheme in mobile cloud computing [J]. International Journal of Computer Applications, 2015, 129 (1): 975-8887.

[13] Li Ruxuan, Shen Chenglin, He Heng, *et al.* A lightweight secure data sharing scheme for mobile cloud computing [J]. IEEE Trans on Cloud Computing, 2017, PP (99): 1-1.

[14] Lyu Maoxu, Li Xuejun, Li Hui. Efficient, verifiable and privacy preserving decentralized attribute-based encryption for mobile cloud computing [C]// Proc of the 2nd IEEE International Conference on Data Science in Cyberspace. [S. l.] : IEEE Computer Society, 2017: 195-204.

[15] Zhao Zhiyuan, Wang Jianhua. Verifiable outsourced ciphertext-policy attribute-based encryption for mobile cloud computing [J]. Ksii Trans on Internet & Information Systems, 2017, 11 (6): 3254-3272.

[16] De S. J, Ruj S. Efficient decentralized attribute based access control for mobile clouds [J]. IEEE Trans on Cloud Computing, 2017, PP (99): 1-1.

[17] 李学俊，吕茂旭．移动云环境下的多授权机构属性基加密方案 [J/OL]. 计算机应用研究, 2018, 35 (5): 1-9. http://www. arocmag. com/article/02-2018-05-006. html. (Li Xuejun and Lyu Maoxu. Multi-authority attribute-based encryption scheme in mobile cloud environment [J/OL]. Application Research of Computers, 2018, 35 (5): 1-9. http://www. arocmag. com/article/02-2018-05-006. html.)

[18] Yang Kan, Jia Xiaohua. Expressive, efficient, and revocable data access control for multi-authority cloud storage [J]. IEEE Trans on Parallel & Distributed Systems, 2014, 25 (7): 1735-1744.

[19] Huang Xiaofang, Tao Qi, Qin Baodong, *et al.* Multi-authority attribute based encryption scheme with revocation [C]// Proc of IEEE International Conference on Computer Communication and Networks. 2015: 1-5.

[20] Cui Hui, Deng R H. Revocable and decentralized attribute-based encryption [J]. Computer Journal, 2016, 59 (8): bxw007.

[21] 张凯，马建峰，李辉，等. 支持高效撤销的多机构属性加密方案 [J]. 通信学报. 2017, 38 (3): 83-91. (Zhang Kai, Ma Jianfeng, Li Hui, *et al*. Multi-authority attribute-based encryption with efficient revocation [J]. Journal on Communications, 2017, 38 (3): 83-91.)

[22] Rouselakis Y, Waters B. Efficient statically-secure large-universe multi-authority attribute-based encryption [C]// Proc of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2015: 315-332.

[23] Beimel A. Secure schemes for secret sharing and key distribution [J]. International Journal of Pure & Applied Mathematics, 1996.

[24] Akinyele J A, Garman C, Miers I, *et al*. Charm: a framework for rapidly prototyping cryptosystems [J]. Journal of Cryptographic Engineering, 2013, 3 (2): 111-128.